IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	James M. Doherty, et al.		
Title:	INTRUSION DETECTION		
App. No.:	10/605,689	Filed:	October 17, 2003
Examiner:	GERGISO, Techane	Group Art Unit:	2137
Customer No.:	60533	Confirmation No.:	2688
Atty. Dkt. No.:	1033-T00534C		

BOARD OF PATENT APPEALS
AND INTERFERENCES
Mail Stop Appeal Brief - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF IN SUPPORT OF APPEAL

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Appellant
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The Real Party in Interest in the present Appeal is AT&T Intellectual Property I, L.P. (formerly known as SBC Knowledge Ventures, L.P.), the assignee, of patent application no. 10/605,689, as evidenced by the assignment set forth at Reel 015014, Frame 0912.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

A. Total Number of Claims in Application

There are 23 claims pending in the application (claims 1-2, 4-16, and 18-25).

B. Status of All the Claims

Claims 1, 10, 15 and 18 are independent claims. According to the Final Office Action dated August 6, 2008 (the "Final Office Action"), claims 1-2, 4-16, and 18-25 stand rejected, and are hereby appealed. Claims 3 and 17 were previously cancelled.

C. Claims on Appeal

There are 23 claims on appeal (claims 1-2, 4-16, and 18-25).

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

The claims hereby Appealed are based on the Amendment filed May 2, 2008. No amendment was offered or entered after the Final Office Action.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The subject matter of claim 1 can be summarized as follows:

A method of detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored. The method includes monitoring data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database. The method further includes, upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, the entry identifying a possible intrusion in a host, and issuing a command to an operating system of the host to bring the host to a single user state.

Claim 1 finds support from at least Figure 2; on page 4, lines 2-15; and on page 9, line 18 to page 10, line 6, of the specification.

The subject matter of claim 10 can be summarized as follows:

A system to detect intrusion including a host running a monitoring daemon working in conjunction with a configuration file for identifying files and directories to be monitored in the host. The host communicates with external networks via one or more network interfaces. The monitoring daemon dynamically monitors files and directories identified by the configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature. The system further includes a digital signature database remote from the host storing the digital signatures associated with files and directories identified by the configuration file. The system further includes a log database remote from the host recording entries corresponding to mismatches between a digital signature stored in the host and a corresponding digital signature in the digital signature database. In the system, a mismatch identifies a possible intrusion in the host resulting in a command being issued to an operating system of the host to bring the host to a single user state

Claim 10 finds support from at least Figures 1 and 2; on page 4, lines 2-15 on page 5, lines 5-15; on page 9, line 18 to page 10, line 6; and on page 12, lines 12-18, of the specification.

The subject matter of claim 15 can be summarized as follows:

An article of manufacture includes a computer usable medium having computer readable program code embedded in the medium to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored. The medium further includes computer readable program code including executable instructions to monitor data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database. The medium further includes computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signatures. The entry identifies a possible intrusion in a host. The medium further includes computer readable program code comprising executable instructions to issue a command to an operating system of the host to bring the host to a single user state upon identifying the mismatch in compared digital signatures.

Claim 15 finds support from at least Figures 1 and 2; on page 10, lines 12-19; and on page 10, line 21 to page 11, line 6, of the specification.

The subject matter of claim 18 can be summarized as follows:

An intrusion detection and isolation method implemented using a monitoring daemon in a host. The host has one or more network interfaces to communicate over one or more networks. The method includes reading a configuration file to identify data entities to be monitored on a host. The method further includes, for each data entity to be monitored, extracting a digital signature from the host. The method further includes, for each data entity to be monitored, querying a remote digital signature database via the one or more network interfaces and requesting a digital signature corresponding to the digital signature extracted from the host. The method further includes, for each data entity to be monitored, receiving the corresponding digital signature from the remote digital signature database. The method further includes matching the digital signature received from the remote digital signature database with the digital signature extracted at the host. The method further includes, upon identifying a mismatch, transmitting an instruction to a

remote log database via one or more of the network interfaces, the instruction executed in the remote log database to record an entry in a log file indicating a possible intrusion in the host. The method further includes issuing a command to an operating system of the host to bring the host to a single user state.

Claim 18 finds support from at least Figures 1 and 2; and on page 7, line 28 to page 9, line 8; and on page 10, lines 12-19 of the specification.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1-2, 4-16 and 18-25, under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 6,647,400 ("Moran"), in view of U.S. Application No. 2002/0129264 ("Rowland"), at page 3 of the Final Office Action.

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

Appellant respectfully appeals each of the rejections applied against all claims now pending on appeal.

Appellant traverses the rejections of claims 1-2, 4-16 and 18-25, under 35 U.S.C. §103(a), as being unpatentable over Moran in view of Rowland

A. Claims 1-2 and 4-9 are Allowable Over Moran and Rowland

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claim 1. For example, the cited portions of Moran and Rowland, alone or in combination, fail to disclose or suggest, upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database where the entry identifies a possible intrusion in a host, and issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1.

The Office admits that Moran fails to teach this feature. *Final Office Action at page 3.* The Office takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses the log handler can accept a variety of

formats and notification can be sent in a number of ways but fails to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can block hosts, users, networks, running commands, logging events, disabling interfaces, disabling a computer, sending email, paging personnel and providing on-screen alerts. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including disabling of the network interfaces, shutdown of active user accounts, locating and logging suspicious activities, notifying a central controller of its actions, requesting collection of forensic evidence, moving between other affected client systems and attempting to contain the intrusion situation. Paragraph 0145 of Rowland mentions shutting down active user accounts. However, shutting down active user accounts is distinct from bringing the host to a single user state. In fact, Rowland appears to be suggesting bringing the host to a zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1.

Paragraph 0148 similarly fails to disclose or suggest issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1. Rather, paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of a known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claim 1. Hence, claim 1 is allowable.

Claims 2 and 4-9 are allowable, at least by virtue of their dependence from an allowable claim. Further, claims 2 and 4-9 recite additional features not disclosed or suggested by the cited portions of Moran and Rowland.

For example, the cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest that a first remote database and a second remote database are located on a single server or a plurality of servers belonging to a local area network, as in claim 4. The Office

takes the position that this feature is disclosed by Rowland at paragraphs 0037, 0053 and 0147. Paragraphs 0037 and 0053 of Rowland were discussed above and fail to disclose or suggest that a first remote database and a second remote database are located on a single server or a plurality of servers belonging to a local area network. Rather, the cited paragraphs simply teach that logging may be done on a remote server but do not disclose or suggest that the first remote database and the second remote database are located on a single server or on a plurality of servers belonging to a local area network. Paragraph 0147 of Rowland discusses a host scanning agent 1304 designed to perform a host vulnerability assessment and vulnerability detection from within the host, but fails to disclose or suggest that the first remote database and the second remote database are located on a single server or at a plurality of servers belonging to a local area network.

B. Claims 10-16 are Allowable Over Moran and Rowland

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claim 10. For example, the cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest a command being issued to an operating system of a host to bring the host to a single user state, as in claim 10.

The Office admits that Moran fails to teach this feature. *Final Office Action at page 3.* The Office takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, simply notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses that the log handler can accept a variety of formats and notification can be sent in a number of ways. Both paragraphs fail to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can issue various commands. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including shutting down active user accounts. However, shutting down active user accounts is distinct from bringing the host to a single user state. In fact, Rowland appears to be suggesting bringing the

host to a zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest a command being issued to an operating system of a host to bring the host to a single user state, as in claim 10.

Paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claim 10. Hence, claim 10 is allowable. Claims 11-14 are allowable, at least by virtue of their dependence from allowable claim 10.

C. Claims 15 and 16 are Allowable Over Moran and Rowland

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claim 15. For example, the cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state, as in claim 15.

The Office admits that Moran fails to teach this feature. *Final Office Action at page 3.* The Office takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, simply notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses that the log handler can accept a variety of formats and notification can be sent in a number of ways. Both paragraphs fail to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can issue various commands. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including shutting down active user accounts. However, shutting down active user accounts is distinct from bringing the host to a single user state. In fact, Rowland appears to be suggesting bringing the

host to a zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state, as in claim 15.

Paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claim 15. Hence, claim 15 is allowable.

Claims 16 is allowable, at least by virtue of its dependence from allowable claim 15.

D. Claims 18-25 are Allowable Over Moran and Rowland

The cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest the specific combination of claim 18. For example, the cited portions of Moran and Rowland, individually or in combination, do not disclose or suggest issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

The Office admits that Moran fails to teach this feature. *Final Office Action at page 3.* The Office takes the position that Rowland teaches this feature at paragraphs 0037, 0053, 0065, 0145 and 0148. Rowland, at paragraph 0037, simply notes that a log handler 203 logs system events locally or remotely. Paragraph 0053 of Rowland discloses the logging handler can accept a variety of formats and notification can be sent in a number of ways. Both paragraphs fail to disclose or suggest bringing a host to a single user state.

Paragraph 0065 describes functionality of an action handler 204 and describes that the action handler 204 can issue various commands. However, paragraph 0065 fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state.

Paragraph 0145 also fails to describe or suggest issuing a command to an operating system of a host to bring the host to a single user state. Paragraph 0145 of Rowland discusses that an intrusion control agent 1302 performs certain functions at a host computer system including shutting down active user accounts. However, shutting down active user accounts is distinct from bringing the host to a single user state. Rowland appears to be suggesting bringing the host to a

zero user state by shutting down the active user accounts. Thus, none of these recited functions disclose or suggest issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

Paragraph 0148 of Roland describes a known intrusion agent 1305 which is designed to specifically look for an alarm on signs of known intrusion. However, nothing in paragraph 0148 discloses or suggests bringing the host to a single user state.

Therefore, the cited portions of Moran and Rowland, individually or in combination, fail to disclose or suggest the specific combination of claim 18. Hence, claim 18 is allowable. Claims 19-25 are allowable, at least by virtual of their dependence from allowable claim 18.

VIII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of each claim involved in the appeal is as follows:

1. (Presently Presented) A method of detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, the method comprising:

monitoring data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database; and

upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host, and issuing a command to an operating system of said host to bring said host to a single user state.

2. (Presently Presented) The method of claim 1, further comprising issuing a command to bring down one or more network interfaces of said host to isolate said host upon identifying the mismatch in compared digital signatures.

3. (Cancelled).

4. (Presently Presented) The method of claim 1, wherein said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network.

5. (Presently Presented) The method of claim 1, wherein communications between said host and first remote database are encrypted.

6. (Presently Presented) The method of claim 1, wherein communications between said host and second remote database are encrypted.

7. (Presently Presented) The method of claim 1, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database.

8. (Presently Presented) The method of claim 1, wherein said second remote database is a SYSLOG database.

9. (Presently Presented) The method of claim 1, wherein said data entities comprise one or more of files, configuration files, and directories.

10. (Presently Presented) A system to detect intrusion comprising:

a host running a monitoring daemon working in conjunction with a configuration file, said configuration file identifying files and directories to be monitored in said host and said host communicating with external networks via one or more network interfaces, said monitoring daemon dynamically monitoring said files and directories identified by said configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature;

a digital signature database remote from said host storing said digital signatures associated with files and directories identified by said configuration file; and

a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database,

wherein a mismatch identifies a possible intrusion in the host, resulting in a command being issued to an operating system of said host to bring said host to a single user state.

11. (Presently Presented) The system of claim 10, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network.

12. (Presently Presented) The system of claim 10, wherein communications between said host and said digital signature database are encrypted.

13. (Presently Presented) The system of claim 10, wherein communications between said host and log database are encrypted.

14. (Presently Presented) The system of claim 10, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database.

15. (Presently Presented) An article of manufacture comprising a computer usable medium having computer readable program code embedded therein to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, said medium comprising:

computer readable program code comprising executable instructions to monitor data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database;

computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signatures, said entry identifying a possible intrusion in a host; and

computer readable program code comprising executable instructions to issue a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures.

16. (Presently Presented) The article of manufacture of 15 further comprising computer readable program code comprising executable instructions to issue a command to bring down one or more network interfaces to isolate said host upon identifying the mismatch in compared digital signatures.

17. (Cancelled).

18. (Presently Presented) An intrusion detection and isolation method implemented using a monitoring daemon in a host, said host having one or more network interfaces to communicate over one or more networks, said method comprising:

reading a configuration file to identify data entities to be monitored on a host;

for each data entity to be monitored, extracting a digital signature from said host;

for each data entity to be monitored, querying a remote digital signature database via said one or more network interfaces and requesting a digital signature corresponding to said digital signature extracted from said host;

for each data entity to be monitored, receiving said corresponding digital signature from said remote digital signature database;

matching digital signature received from said remote digital signature database with digital signature extracted at said host;

upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log

database to record an entry in a log file indicating a possible intrusion in said host; and

issuing a command to an operating system of said host to bring said host to a single user state.

19. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network.

20. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein communications between said host and digital signature database are encrypted.

21. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein communications between said host and log database are encrypted.

22. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein said digital signature database is an MD5 database.

23. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein said log database is a SYSLOG database.

24. (Presently Presented) The intrusion detection and isolation method of claim 18, wherein said data entities are any of the following: system files, configuration files, or directories.

25. (Presently Presented) The intrusion detection and isolation method of claim 18, further comprising issuing a command to bring down said one or more network interfaces to isolate said host.

IX. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

(N/A)

X. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

(N/A)

XI. CONCLUSION

For at least the above reasons, all pending claims are allowable and a notice of allowance is courteously solicited. Please direct any questions or comments to the undersigned attorney at the address indicated. Appellant respectfully requests reconsideration and allowance of all claims and that this patent application be passed to issue.

Respectfully submitted,

12-5-2008
Date

Jeffrey G. Toler; Reg. No. 38,342
Attorney for Appellant(s)
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)